

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2004 年 5 月 13 日 (13.05.2004)

PCT

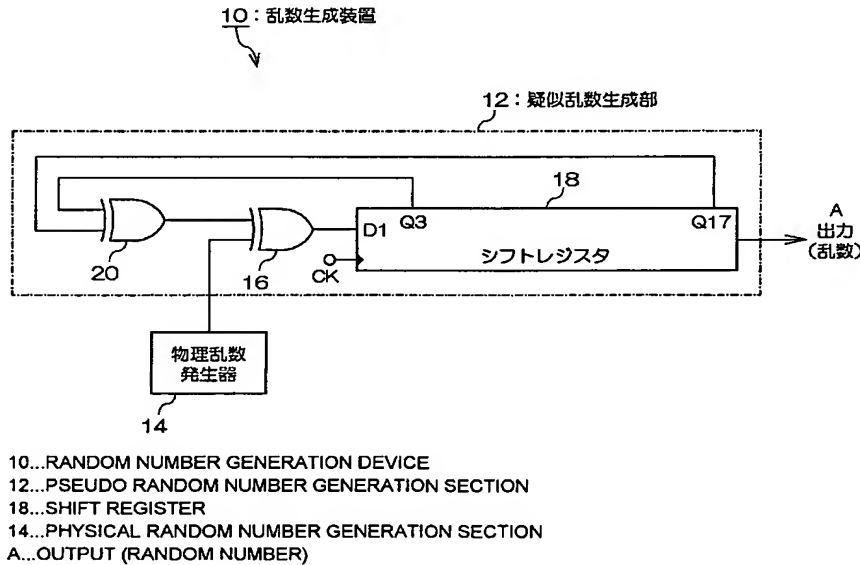
(10) 国際公開番号  
WO 2004/040838 A1

- (51) 国際特許分類<sup>7</sup>: H04L 9/24, G06F 7/58 KAISHA SURI SEKKEI KENKYUSHO) [JP/JP]; 〒371-0816 群馬県 前橋市上佐鳥町 5 4-2 Gunma (JP).
- (21) 国際出願番号: PCT/JP2003/014055
- (22) 国際出願日: 2003 年 11 月 4 日 (04.11.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願2002-320035 2002 年 11 月 1 日 (01.11.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO.,LTD.) [JP/JP]; 〒570-8677 大阪府 守口市京阪本通 2 丁目 5 番 5 号 Osaka (JP). 株式会社数理設計研究所 (KABUSHIKI
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてののみ): 女屋 正人 (ON-AYA,Masato) [JP/JP]; 〒570-8677 大阪府 守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内 Osaka (JP). 玉置 晴朗 (TAMAKI,Haruro) [JP/JP]; 〒371-0816 群馬県 前橋市上佐鳥町 5 4-2 株式会社数理設計研究所内 Gunma (JP). 池谷 昭 (IKETANI,Akira) [JP/JP]; 〒110-0005 東京都 台東区上野 1 丁目 1 9 番 1 0 号 三洋セミコンデバイス株式会社内 Tokyo (JP).
- (74) 代理人: 吉田 研二, 外 (YOSHIDA,Kenji et al.); 〒180-0004 東京都 武蔵野市吉祥寺本町 1 丁目 3 4 番 1 2 号 Tokyo (JP).
- (81) 指定国 (国内): CN, KR, US.

[続葉有]

(54) Title: RANDOM NUMBER GENERATION DEVICE

(54) 発明の名称: 乱数生成装置



(57) Abstract: A random number generation device includes a pseudo random number generation section capable of outputting a plurality of random numbers of different pseudo random number series, a physical random number generation section for generating a physical random number, and a switching section for switching the pseudo random number series of the random numbers output from the pseudo random number generation section according to the physical random number generated by the physical random number generation section. The output of the pseudo random number generation section is used as an output random number. Since a plurality of different pseudo random number series are switched to be output by a physical random number, it is possible to reduce the predictability of the random number as compared to the conventional random number generation device using only a pseudo random number. Moreover, since the physical random number is not directly used as an output random number, even if any operation is added to the physical random number generation means from outside, the affect for the predictability of the output random number is significantly lowered as compared to the conventional device.

[続葉有]



(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

(57) 要約: 乱数生成装置は、複数の異なる疑似乱数系列の乱数を出力可能な疑似乱数生成部と、物理乱数を生成する物理乱数発生器と、物理乱数発生器の生成した物理乱数に基づいて疑似乱数生成部の出力する乱数の疑似乱数系列を切り替える切替部と、を備え、疑似乱数生成部の出力を出力乱数とする。複数の異なる疑似乱数系列を物理乱数によって切り替えて出力するため、従来の疑似乱数のみを用いた乱数生成装置に比べて乱数の予測性を低減することができる。また、物理乱数を直接的な出力乱数としては用いないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測性に対する影響は従来装置に比べてかなり小さくなる。

## 明 細 書

## 乱数生成装置

## 技術分野

本発明は、乱数生成装置に関し、特に暗号化アルゴリズムに好適な乱数生成装置に関する。

## 背景技術

暗号化アルゴリズム等では、セキュリティの確保のために、しばしば乱数が用いられる。その場合の乱数としては、一般的に、M系列（Maximum length code：最長符号系列）等に代表される疑似乱数が用いられてきた。M系列符号は、公知の線形シフトレジスタ符号発生器によって生成することができる。

また、上記疑似乱数以外の乱数として、原子核の崩壊現象がランダムとなることや電気雑音等の自然現象を利用して生成される物理乱数が知られている。暗号化アルゴリズム等においても、上記疑似乱数に替えて、この物理乱数を利用する場合もある（例えば、日本特開2000-66592公報参照。）

しかしながら、M系列等に代表される疑似乱数は、必ずしも安全性の高い乱数とは言えず、セキュリティ確保の面からは好ましくないところがある。疑似乱数は、一定の算術プロセスあるいは関数の組み合わせから生成されるため、同じ初期条件を与えれば同一の値となり、乱数の推定が可能となるからである。

また、一般的に物理乱数は微弱な信号であるため、暗号化アルゴリズム等で使用するためには、通常、増幅器によって利用可能なレベルに増幅される。ところが、これら全体は電界や磁界によって影響を受ける場合があり、それらの意図的または意図せざる印加によって乱数の発生確率が操作され、安全性が低下してしまう場合があった。

## 発明の開示

本発明にかかる乱数生成装置は、複数の異なる疑似乱数系列の乱数パターンを

出力可能な疑似乱数生成手段と、物理乱数を生成する物理乱数生成手段と、上記物理乱数生成手段の生成した物理乱数に基づいて上記疑似乱数生成手段の出力する乱数の疑似乱数系列を切り替える切替手段と、を備える。すなわち、上記本発明にかかる乱数生成装置によれば、複数の異なる疑似乱数を物理乱数によって切り替えて出力するため、従来の疑似乱数のみを用いた乱数生成装置に比べて乱数の予測性を低減することができる。また、物理乱数を直接的な出力乱数としては用いていないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測性に対する影響は従来装置に比べてかなり小さくなる。

上記本発明にかかる乱数生成装置は、種々の形態によって実現することができる。例えば、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段が、線形シフトレジスタ符号発生器を含み、上記切替手段が、上記線形シフトレジスタ符号発生器への帰還入力値の反転／非反転を、上記物理乱数生成手段によって生成された物理乱数に基づいて切り替えるよう、構成することができる。

また、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、上記切替手段は、上記線形シフトレジスタ符号発生器からの出力値の反転／非反転を、上記物理乱数生成手段によって生成された物理乱数に基づいて切り替えるよう、構成することができる。

また、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段が、線形シフトレジスタ符号発生器を含み、該線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく複数の帰還入力値を生成し、上記切替手段が、上記生成された複数の帰還入力値のうち該線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、上記物理乱数生成手段で生成された物理乱数に基づいて切り替えるよう、構成することができる。

また、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段が、所定のタップの組み合わせに基づく第一の帰還入力値を生成する線形シフトレジスタ符号発生器と、該第一の帰還入力値を受け取り上記線形シフトレジスタ符号発生器と同期して所定ビット数ビットシフトを行いその出力を第二の帰還入力値とするフリップフロップと、を含み、上記切替手段が、上記第一または第二の帰還入力値のうち上記線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、上記

物理乱数生成手段で生成された物理乱数に基づいて切り替えるよう、構成することができる。

また、上記本発明にかかる乱数生成装置では、上記線形シフトレジスタ符号発生器の符号列を検出する検出手段を備え、上記切替手段は、有効なまたは切り替えによって有効となる疑似乱数系列の乱数が上記検出された符号列によっては生成不能である場合には、該疑似乱数系列以外の疑似乱数系列に切り替えるのが好適である。これにより、線形シフトレジスタ符号発生器において有効な疑似乱数系列に対して疑似乱数の生成されない符号列となるのが抑制される。

また、上記本発明にかかる乱数生成装置では、上記線形シフトレジスタ符号発生器の符号列を検出する検出手段と、有効なまたは切り替えによって有効となる疑似乱数系列の乱数が上記検出された符号列によっては生成不能である場合には、上記符号列のビット値のうち少なくとも一つを反転させるのが好適である。このような構成によっても、線形シフトレジスタ符号発生器において有効な疑似乱数系列に対して疑似乱数の生成されない符号列となるのが抑制される。

#### 図面の簡単な説明

図 1 は、本発明の実施の形態 1 にかかる乱数生成装置の構成図である。

図 2 は、本発明の実施の形態 1 にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

図 3 は、本発明の実施の形態 1 にかかる物理乱数発生器の構成図である。

図 4 は、本発明の実施の形態 2 にかかる乱数生成装置の構成図である。

図 5 は、本発明の実施の形態 3 にかかる乱数生成装置の構成図である。

図 6 は、本発明の実施の形態 3 にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

図 7 は、本発明の実施の形態 4 にかかる乱数生成装置の構成図である。

図 8 は、本発明の実施の形態 4 にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

図 9 は、本発明の実施の形態 5 にかかる乱数生成装置の構成図である。

図 10 は、本発明の実施の形態 5 にかかる乱数生成装置によって生成される疑似

似乱数系列の一例を示す図である。

図 1 1 は、本発明の実施の形態 6 にかかる乱数生成装置の構成図である。

発明を実施するための最良の形態

実施の形態 1. 図 1 は本実施形態にかかる乱数生成装置 1 0 の構成図、図 2 は乱数生成装置 1 0 によって生成される二つの M 系列の巡回パターンを示す図、また図 3 は物理乱数発生器 1 4 の構成図である。

乱数生成装置 1 0 は、疑似乱数生成部 1 2、物理乱数発生器 1 4、および切替部 1 6 を含む。このうち疑似乱数生成部 1 2 は、少なくとも一つの線形シフトレジスタ符号発生器を含み、複数の異なる疑似乱数系列（例えば、M 系列等）の乱数パターンを出力することができる。本実施形態では、縦続して接続された複数のフリップフロップを含むシフトレジスタ 1 8 と、所定の複数のタップ位置からの出力値の排他的論理和を出力する EXOR ゲート 2 0 と、が設けられており、これらにより、M 系列の乱数を出力する線形シフトレジスタ符号発生器が構成されている。図 1 の例では、シフトレジスタ 1 8 は、1 7 個のフリップフロップを有しクロック（CK）に応じてビットシフトする 1 7 段シフトレジスタとして構成され、入力側より第 3 番目と第 1 7 番目のフリップフロップからのタップ出力（Q 出力；Q 3，Q 1 7）に基づいて帰還入力値（シフトレジスタ 1 8 の D 1 入力；「1」（ハイレベル）または「0」（ローレベル））が生成される。

一般的な線形シフトレジスタ符号発生器では、EXOR ゲート 2 0 の出力がそのままシフトレジスタ 1 8 に帰還入力されるが、本実施形態では、EXOR ゲート 2 0 の出力は切替部 1 6 を経由してシフトレジスタ 1 8 に入力される。切替部 1 6 は、物理乱数発生器 1 4 からの物理乱数出力（バイナリコード）に基づいて、帰還入力値となる EXOR ゲート 2 0 からの出力値の反転／非反転を切り替える。すなわち、この物理乱数出力は、切替制御信号とすることができる。図 1 の例では、切替部 1 6 は、EXOR ゲートとして構成される。EXOR ゲートは、二つの入力値が不一致であるときに「1」を出力し、一致するときに「0」を出力する。したがって、物理乱数出力値が「1」であるときは、切替部 1 6 において EXOR ゲート 2 0 の出力値は反転され、他方、物理乱数出力値が「0」であると

きは、反転されない。つまり、切替部 16 は、物理乱数出力値に応じて、E X O R ゲート 20 からの出力値を反転して帰還入力値とするか、あるいは反転させずにそのまま帰還入力値とするかを、切り替えていることになる。

このような切替部 16 の動作により、疑似乱数生成部 12 は、異なる二つの疑似乱数系列を生成することができる。図 1 の例では、物理乱数出力値が「0」であるときは切替部 16 において帰還入力値は反転されないから、疑似乱数生成部 12 においてクロック信号 (CK) に基づいて  $2^{17}-1$  サイクルで循環的に変化する M 系列 1-1 (図 2 (a)) が生成され、他方、物理乱数出力値が「1」であるときは、切替部 16 において帰還入力値が反転されるから、同じくクロック信号に基づいて  $2^{17}-1$  サイクルで循環的に変化する M 系列 1-2 (図 2 (b)) が生成される。なお、M 系列 1-1 と M 系列 1-2 とは、変化のパターンは同一であるが、符号が互いに逆となっており、異なる疑似乱数系列として取り扱うことができる。これにより、切替部 16 に与える切替信号が物理乱数で制御されるので、一方の疑似乱数系列を生成するシフトレジスタの途中情報を用いて、他方の疑似乱数系列から一方の疑似乱数系列に切り替えることにより、予測不可能な疑似乱数系列となる。また、二つの疑似乱数系列の「0」と「1」の頻度がそれぞれ  $2^{16}-1$  および  $2^{16}$  と、 $2^{16}$  および  $2^{16}-1$  の対称比率になるので、二つの疑似乱数系列を物理乱数によって切り替え制御すれば、「0」と「1」の頻度分布状態が理想状態に近づくという効果もある。

図 3 に示すように、物理乱数発生器 14 は、物理乱数発生源 14 a、増幅回路 14 b および二値化回路 14 c を備える。このうち、物理乱数発生源 14 a は、自然現象に基づいてランダムに変化する信号を生じうるものであり、例えば、上記特許文献 1 に開示されるような、接合を含む電流路に生じる雑音信号を生じる半導体素子を含むものとすることができる。なお、これには限られず、放射性物質の崩壊を利用したもの等もこの物理乱数発生源 14 a として用いることができる。物理乱数発生源 14 a にて生じた信号は、増幅回路 14 b において増幅され、さらに二値化回路 14 c において二値化処理される。二値化回路 14 c は、所定のサンプリングタイミングで、増幅された信号の振幅と所定の閾値とを比較し、例えば、増幅された信号の振幅が所定の閾値より高いときには「1」を、逆に低

いときには「0」を出力する。こうして物理乱数発生器14により、「1」または「0」を示す所定電圧の物理乱数出力値が生成される。なお、二値化回路14cにおける閾値のレベルは任意に設定することができるが、通常は「1」および「0」の発生確率がほぼ1対1となるように設定される。なお、二値化回路14cにおいて、単に、増幅された信号の振幅を所定の閾値と比較して出力信号を発生するようにしてもよい。

このように、本実施形態にかかる乱数発生装置10では、二つの異なる疑似乱数系列のうちどちらを出力するかを、物理乱数によって切り替えるだけでなく、シフトレジスタの途中情報を有効に利用して二つの疑似乱数系列の帰還状態を変化させている。こうすることで、疑似乱数のみを用いた場合に比べて、乱数の予測が難しくなる。また、物理乱数を直接的な出力乱数としては用いないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測性に対する影響は従来装置に比べてかなり小さくなる。

実施の形態2. 図4は本実施形態にかかる乱数生成装置30の構成図である。乱数生成装置30は、疑似乱数生成部32、物理乱数発生器14、および切替部36を含む。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態にかかる疑似乱数生成部32では、線形シフトレジスタ符号発生器からの出力値を、切替部36によって反転または非反転して出力乱数とする。図4の例では、シフトレジスタ18およびEXORゲート20を含む典型的な線形シフトレジスタ符号発生器が構成されており、シフトレジスタ18の所定ビット（例えば第17番目のビット）のQ出力およびQb出力（Q出力の反転出力）がそれぞれ切替部36に入力される。

切替部36は、二つのANDゲート36a、36bを備えており、そのうち一方のANDゲート36aには、Qb出力と物理乱数発生器14からインバータ36cを介して物理乱数出力が入力され、もう一方のANDゲート36bには、Q出力と物理乱数発生器14からの物理乱数出力が入力される。そして、これら二つのANDゲート36a、36bの出力がORゲート36dに入力され、このORゲート36dの出力が出力乱数となる。



**UTILITY/CIP APPLICATION CHECKLIST**

**Client/Matter Number:** 04995/216001  
**Client/Matter Name:** NGB / Hard Disk Recorder and Video Record Apparatus

---

**IPDAS (Mandatory)**

- |  |  |   |                                      |
|--|--|---|--------------------------------------|
| <input type="checkbox"/> Transmittal – Utility Application | <input type="checkbox"/> Application Cover Sheet | <input type="checkbox"/> Application Data Sheet | <input type="checkbox"/> Declaration |
| <input type="checkbox"/> Postcard                          | <input type="checkbox"/>                         | <input type="checkbox"/>                        | <input type="checkbox"/>             |

**IPDAS (As Needed)**

- |   |   |   |  |
|---|---|---|--|
| <input type="checkbox"/> Fee Transmittal                  | <input type="checkbox"/> Assignment                                     | <input type="checkbox"/> Assignment Recordation Coversheet            | <input type="checkbox"/> Preliminary Amendment   |
| <input type="checkbox"/> Information Disclosure Statement | <input type="checkbox"/> Claim for Priority and Submission of Documents | <input type="checkbox"/> Check Request/Credit Card Authorization Form | <input type="checkbox"/> Non-Recordation Request |
| <input type="checkbox"/> IDS Citation by Applicant        | <input type="checkbox"/>  | <input type="checkbox"/>  | <input type="checkbox"/>                         |

**APPLICATION FILE**

- ☐ If CIP, parent case is COMPLETE and PENDING. A Response to Missing Parts, and/or Petition for Extension has been filed. All outstanding rejections in the parent case have been answered
- ☐ Cover sheet includes: title, names of ALL inventors, Express Mail stamp, and PTO Customer No. label.
- ☐ Specification pages are present and checked for printer errors. Number of pages: \_\_\_\_\_
- ☐ All figures are included and checked against the list of figures in the specification. Number of sheets: \_\_\_\_\_
- ☐ At least one claim is included. Number of claims: \_\_\_\_\_ total / \_\_\_\_\_ independent
- ☐ Application has been reviewed to ensure all pages and figures are present. Claims have been reviewed by WA for obvious informalities.
- ☐ Transmittal letter is complete and accurate, names ALL inventors, includes Express Mail stamp and PTO Customer No. label.
- ☐ Declaration and Power of Attorney is signed/unsigned (circle one), and PTO Customer No. label is attached.
- ☐ Check / Credit Card Authorization Form (circle one) for application fee is included. Amount: \_\_\_\_\_
- ☐ If filed, an IDS letter and PTO Form SB-08 are complete and accurate, and PTO Customer No. label is attached. If an IDS is not filed with the application, a docketing entry has been entered for 3-months after filing date.
- ☐ Original invention disclosure has been reviewed for additional prior art and other §102 events.
- ☐ If filed, an assignment package contains a recordation cover sheet and all information is complete and accurate.
- ☐ Express Mail Declarations include: correct Mailing Label Number and is addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
- ☐ Postcard lists express mail number, all papers being sent and the number of pages of each.
- ☐ WA has reviewed file, I-Manage, and e-mail to remove all work copies, notes and prior drafts.
- ☐ If convention application, WA has reviewed claim for obvious informalities.

☐ Assistant

☐ Double-checker

Application filing package is substantively correct, complete, and complies with all client instructions.

△ (WA Initials)

I have reviewed and approved the filing.

(AL Initials)

この切替部 36 により、物理乱数出力に応じて Q 出力あるいは Q b 出力のうちいずれか一方が有効となる。すなわち物理乱数出力値が「1」のときは、AND ゲート 36 a の出力値は必ず「0」となり、かつ AND ゲート 36 b の出力値は Q b 出力値と同じになるので、乱数出力値は Q b 出力値と同じになる。逆に物理乱数出力値が「0」のときは、AND ゲート 36 b の出力値は必ず「0」となり、かつ AND ゲート 36 a の出力値は Q 出力値と同じになるので、乱数出力値は Q 出力値と同じになる。すなわち、切替部 36 の作用により、物理乱数出力値が「1」であるときは、Q 出力値を反転した値が出力乱数となり、逆に物理乱数出力が「0」であるときは、Q 出力値がそのまま出力乱数となっている。したがって、本実施形態にかかる乱数生成装置 30 も、上記実施の形態 1 と同様に、図 2 に示した二つの乱数系列 (M 系列 1-1, 1-2) を、物理乱数によって切り替えて出力することができる。すなわち、このような構成によっても、上記実施の形態 1 と同様の効果が得られる。

実施の形態 3. 図 5 は本実施形態にかかる乱数生成装置 40 の構成図、また図 6 は、乱数生成装置 40 によって生成される二つの M 系列の巡回パターンを示す図である。乱数生成装置 40 は、疑似乱数生成部 42、物理乱数発生器 14、および切替部 46 を含む。なお、ここでも、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態にかかる疑似乱数生成部 42 では、線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく二種類の帰還入力値を生成することができる。そして、EXOR ゲート 20 b の出力の通過／遮断を物理乱数によって決定している。具体的には、図 5 の例では、線形シフトレジスタ符号発生器として、シフトレジスタ 18 と、異なるタップ出力の組み合わせについてそれぞれ排他的論理和を出力する複数の EXOR ゲート 20 a, 20 b, 20 c とが設けられる。EXOR ゲート 20 a は、シフトレジスタ 18 の入力側より第 3 番目と第 17 番目のタップ出力 (Q 3, Q 17) の排他的論理和を出力し、EXOR ゲート 20 b は、シフトレジスタ 18 の入力側より第 1 番目と第 2 番目のタップ出力 (Q 1, Q 2) の排他的論理和を出力する。EXOR ゲート 20 a の出力は直接 EXOR ゲート 20 c に入力されるが、EXOR ゲート 20 b の出力は AND ゲート (切

替部) 46 を介して EXOR ゲート 20c に入力される。AND ゲート 46 には、物理乱数発生器 14 からの物理乱数出力が入力される。

この構成では、物理乱数出力値が「1」である場合には、AND ゲート 46 の出力値は EXOR ゲート 20b の出力値と同じになるから、EXOR ゲート 20c からは、シフトレジスタ 18 への帰還入力値として、EXOR ゲート 20a の出力値と EXOR ゲート 20b の出力値との排他的論理和が出力されることになる。他方、物理乱数出力値が「0」である場合には、AND ゲート 46 の出力値は必ず「0」となるから、EXOR ゲート 20c からの出力値は、EXOR ゲート 20a の出力値と同じになる。つまり、物理乱数出力値が「0」であるときはタップ出力 (Q3, Q17) に基づく帰還入力値が有効となるから、疑似乱数生成部 12 において M 系列 3-1 (図 6(a)) が生成され、他方、物理乱数出力値が「1」であるときは、タップ出力 (Q1, Q2, Q3, Q17) に基づく帰還入力値が有効となるから、M 系列 3-2 (図 6(b)) が生成される。このように、本実施形態にかかる乱数生成装置 40 も、二つの乱数系列 (M 系列 3-1, 3-2) を、物理乱数によって切り替えて出力することができる。

実施の形態 4. 図 7 は本実施形態にかかる乱数生成装置 50 の構成図、また図 8 は、乱数生成装置 50 によって生成される三つの M 系列の巡回パターンを示す図である。乱数生成装置 50 は、疑似乱数生成部 52、物理乱数発生器 14、および切替部 56 を含む。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態にかかる疑似乱数生成部 52 では、線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく三種類の帰還入力値を生成することができる。そして、それら三種類の帰還入力値のうちどれを有効とするかを、物理乱数によって決定している。具体的には、図 7 の例では、線形シフトレジスタ符号発生器として、シフトレジスタ 18 と、異なるタップ出力の組み合わせに基づく入力値の排他的論理和を出力する複数の EXOR ゲート 20a, 20b, 20c, 20d とが設けられる。EXOR ゲート 20a は、シフトレジスタ 18 の入力側より第 3 番目と第 17 番目のタップ出力 (Q3, Q17) の排他的論理和を出力し、EXOR ゲート 20b は、シフトレジスタ 18 の入力側より第 1 番目と第 2

番目のタップ出力（Q 1， Q 2）の排他的論理和を出力し、また EXOR ゲート 20 c は、シフトレジスタ 18 の入力側より第 4 番目と第 7 番目のタップ出力（Q 4， Q 7）の排他的論理和を出力する。EXOR ゲート 20 a の出力は直接 EXOR ゲート 20 d に入力されるが、EXOR ゲート 20 b， 20 c の出力は、それぞれ AND ゲート 56 b， 56 c および OR ゲート 56 d を介して EXOR ゲート 20 d に入力される。また AND ゲート 56 b， 56 c には、三分周器 56 a からの出力が入力される。

本実施形態では、三分周器 56 a、AND ゲート 56 b， 56 c および OR ゲート 56 d が、切替部 56 として機能する。この構成において、公知の構成を有する三分周器 56 a は、物理乱数発生器 14 からの物理乱数出力をクロックとして、その Q 1 出力値および Q 2 出力値を、「0」，「0」（パターン 1）、「0」，「1」（パターン 2）、「1」，「0」（パターン 3）の三パターンで巡回的に更新する。そしてパターン 1、すなわち Q 1 出力値：「0」、Q 2 出力値：「0」のときは、OR ゲート 56 d の出力値は「0」となり、この場合には、EXOR ゲート 20 a の出力値が、シフトレジスタ 18 に帰還入力値として入力される。同様にパターン 2、すなわち Q 1 出力値：「1」、Q 2 出力値：「0」のときは、OR ゲート 56 d の出力値は、EXOR ゲート 20 b の出力値と同じになる。したがってこの場合には、EXOR ゲート 20 d からは、シフトレジスタ 18 への帰還入力値として、EXOR ゲート 20 a の出力値と EXOR ゲート 20 b の出力値との排他的論理和が出力される。またパターン 3、すなわち Q 1 出力値「1」、Q 2 出力値：「0」のときは、OR ゲート 56 d の出力値は、EXOR ゲート 20 c の出力と同じ値となる。したがってこの場合には、EXOR ゲート 20 d からは、シフトレジスタ 18 への帰還入力値として、EXOR ゲート 20 a の出力値と EXOR ゲート 20 c の出力値との排他的論理和が出力される。つまり、物理乱数出力が更新されるたびに、疑似乱数生成部 12 において、[1] EXOR ゲート 20 a に入力されるタップ出力（Q 3， Q 17）に基づく帰還入力値が有効となる M 系列 4-1（図 8（a））、[2] EXOR ゲート 20 a， 20 b に入力されるタップ出力（Q 1， Q 2， Q 3， Q 17）に基づく帰還入力値が有効となる M 系列 4-2（図 8（b））、および [3] EXOR ゲート 20 a， 20 c に入力されるタップ出力（Q

3, Q 4, Q 7, Q 1 7) に基づく帰還入力値が有効となるM系列 4-3 (図 8 (c)) が生成される。このように、本実施形態にかかる乱数生成装置 5 0 は、三つの乱数系列 (M 系列 4-1, 4-2, 4-3) を、物理乱数によって切り替えて出力することができる。

実施の形態 5. 図 9 は本実施形態にかかる乱数生成装置 6 0 の構成図、また図 1 0 は、乱数生成装置 6 0 によって生成される二つのM系列の巡回パターンを示す図である。乱数生成装置 6 0 は、疑似乱数生成部 6 2、物理乱数発生器 1 4、および切替部 6 6 を含む。なお、ここでも、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態にかかる疑似乱数生成部 6 2 は、帰還入力を得るタップ (帰還入力の元となるタップ) は同一とし、シフトレジスタのビット数を変更するように構成されており、該シフトレジスタのビット数の変更を物理乱数によって決定している。具体的には、図 9 の例では、線形シフトレジスタ符号発生器として、1 5 段のシフトレジスタ 6 8 と、縦続に配置された二つのフリップフロップ 6 2 a, 6 2 b と、所定のタップ出力の組み合わせについて排他的論理和を出力する EX OR ゲート 2 0 e とが設けられる。EX OR ゲート 2 0 e は、シフトレジスタ 6 8 の入力側より第 1 番目と第 1 5 番目のタップ出力 (Q 1, Q 1 5) の排他的論理和を出力する。EX OR ゲート 2 0 e の出力は、前段側のフリップフロップ 6 2 a と、AND ゲート 6 6 a とに入力される。

切替部 6 6 は、二つの AND ゲート 6 6 a, 6 6 b を備えており、そのうち一方の AND ゲート 6 6 a には、EX OR ゲート 2 0 e の出力と物理乱数発生器 1 4 からの物理乱数出力が入力され、もう一方の AND ゲート 6 6 b には、Q 出力と物理乱数発生器 1 4 からインバータ 6 6 c を介して物理乱数出力が入力される。そして、これら二つの AND ゲート 6 6 a, 6 6 b の出力が OR ゲート 6 6 d に入力され、この OR ゲート 6 6 d の出力がシフトレジスタ 6 8 に入力される。

この切替部 6 6 により、物理乱数出力に応じて、EX OR ゲート 2 0 e の出力あるいはフリップフロップ 6 2 b の出力のうちいずれか一方が有効となる。すなわち物理乱数出力値が「0」のときは、AND ゲート 6 6 a の出力値は必ず「0」となり、かつ AND ゲート 6 6 b の出力値はフリップフロップ 6 2 b の出力値と

同じになるから、ORゲート66dの出力値はフリップフロップ62bの出力値と同じになる。逆に物理乱数出力値が「1」のときは、ANDゲート66bの出力は必ず「0」となり、かつANDゲート66aの出力値はEXORゲート20eの出力値と同じになるから、ORゲート66dの出力値はEXORゲート20eの出力値と同じ値となる。すなわち、切替部66の作用により、物理乱数出力値が「0」であるときは、フリップフロップ62a、62bもシフトレジスタの一部として機能することになり、これらを含めた17段のシフトレジスタによって、タップ出力(Q3, Q17)に基づく帰還入力値が有効となるM系列5-1(図10(a))が生成される。他方、物理乱数出力が「1」であるときは、フリップフロップ62a、62bは無効となり、15段のシフトレジスタ68によって、タップ出力(Q1, Q15)に基づく帰還入力値が有効となるM系列5-2(図10(b))が生成される。このように、本実施形態にかかる乱数発生装置60は、段数の異なる二つのシフトレジスタによって発生される乱数系列(M系列5-1, 5-2)を、物理乱数によって切り替えて出力することができる。

実施の形態6. 図11は本実施形態にかかる乱数生成装置70の構成図である。乱数生成装置70は、疑似乱数生成部72、物理乱数発生器14、および切替部16を含む。本実施形態の疑似乱数生成部72は、シフトレジスタ78(18)内に後述する検出回路78aが設けられている点を除いては実施の形態1の疑似乱数生成部12と同じであり、図2に示すM系列1-1, 1-2を生成することができる。なお、ここでも、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

線形シフトレジスタ符号発生器は、シフトレジスタ内の符号列によっては、M系列符号を生成できない。例えば、シフトレジスタの全ビットの値が「0」である場合にはM系列1-1を生成することができないし、また、シフトレジスタの全ビットが「1」である場合にはM系列1-2を生成することができない。一の疑似乱数系列の符号のみを生成する従来の一般的な線形シフトレジスタ符号発生器では、例えば初期値をそのような符号列としないように留意すれば十分であったが、上記実施形態のように、生成される疑似乱数系列が動作中に変更される場合には、有効な疑似乱数系列に対してシフトレジスタ内の符号列が該系列を生じ

ないものとならないようにするための対策を講じておくのが望ましい。そのために、本実施形態にかかる乱数生成装置 70 は、上記実施の形態 1 にかかる乱数生成装置 10 に、検出回路 78 a、78 b、AND ゲート 82 a、82 b、フリップフロップ 84 a、84 b、およびフリップフロップ 80 を付加した構成となっている。

上記付加的な構成要素について説明する。物理乱数発生器 14 からの出力（物理乱数出力）は、フリップフロップ 80 に入力される。なお、本実施形態でも、物理乱数出力値「0」は M 系列 1-1（図 2（a））を、また「1」は M 系列 1-2（図 2（a））を示すものとして規定されている。検出回路 78 a は、シフトレジスタ 78 の全ビットの値が「1」であるときに、AND ゲート 82 a に「1」を出力する（例えば全ビットの値の論理積を出力する）。また検出回路 78 b は、シフトレジスタ 78 の全ビットの値が「0」であるときに、AND ゲート 82 b に「1」を出力する（例えば全ビットの反転値の論理積を出力する）。AND ゲート 82 a には、検出回路 78 a の出力とフリップフロップ 80 の Q 出力とが入力され、その出力はフリップフロップ 84 a に入力される。AND ゲート 82 b には、検出回路 78 b の出力とフリップフロップ 80 の Q b 出力とが入力され、その出力はフリップフロップ 84 b に入力される。そして、フリップフロップ 84 a の出力はリセット信号（R 入力）として、またフリップフロップ 84 b の出力はセット信号（S 入力）として、フリップフロップ 80 に入力される。なお、図 11 の例では、検出回路 78 a、78 b はシフトレジスタ 78 に内蔵されているが、これらをシフトレジスタ 78 の外部に接続してもよい。

上記構成において、シフトレジスタ 78 の全ビットの値が「1」であるときに、物理乱数出力値が「0」から「1」に変化すると、フリップフロップ 80 の値は「1」となり、Q 出力値が「1」となる。また、検出回路 78 a の出力値は「1」であるから、AND ゲート 82 a の出力値は「1」となる。そして、フリップフロップ 84 a の値が「1」となって、フリップフロップ 80 にリセット信号が入力される。したがって、この場合、フリップフロップ 80 の値は「1」から「0」に変更される。すなわち上記構成によれば、シフトレジスタ 78 において M 系列 1-1（図 2（a））の符号が生じない状態（すなわち全ビットの値が「0」）と

なるのを防止することができる。

一方、シフトレジスタ78の全ビットの値が「0」であるときに、物理乱数出力値が「1」から「0」に変化すると、フリップフロップ80の値が「0」となり、Qb出力値が「1」となる。また、検出回路78bの出力値は「1」であるから、ANDゲート82bの出力値は「1」となる。そして、フリップフロップ84bの値が「1」となって、フリップフロップ80にセット信号が入力される。したがって、この場合、フリップフロップ80の値は「0」から「1」に変更される。すなわち上記構成によれば、シフトレジスタ78においてM系列1-2(図2(b))の符号が生じない状態(すなわち全ビットの値が「1」)となるのを防止することができる。

なお、フリップフロップ84a, 84bの出力により、シフトレジスタ78の少なくとも一つのビットの値を変化させるようにしても同様の効果が得られる。例えば、フリップフロップ84aの出力を、シフトレジスタ78内を構成する少なくとも一つのフリップフロップのリセット信号とすれば、当該フリップフロップ(ビット)の値が「0」となるので、M系列1-1の符号を生じない状態となるのを防止することができる。また、フリップフロップ84bの出力をシフトレジスタ78内を構成するいずれかのフリップフロップのリセット信号とすれば、当該フリップフロップ(ビット)の値が「1」となるので、M系列1-2の符号を生じない状態となるのを防止することができる。

以上、本発明の好適な実施形態について説明したが、本発明は上記実施形態で示した構成には限定されず、種々の等価回路によっても実施可能である。上記実施形態では、疑似乱数が、17段または15段のシフトレジスタを有する線形シフトレジスタ符号発生器によって生成される数種類のM系列符号である場合を例示したが、これには限定されず、それ以外の段数のシフトレジスタあるいはタップの組み合わせに基づくM系列であってもよい。また、上記実施の形態6は、上記実施の形態1を基礎としたものを例示的に示したが、他の実施形態に対しても同様に適用可能であることは言うまでもない。また、上記実施の形態1, 3~6では、シフトレジスタの最終段のフリップフロップからの出力を乱数出力としたが、他のフリップフロップからの出力を乱数出力としてもよいし、シフトレジス



タに入力される帰還値を乱数出力としてもよい。

#### 産業上の利用可能性

以上説明したように、本発明によれば、複数の疑似乱数系列のうちどれを有効とするかを物理乱数によって切り替えるため、その予測が難しく暗号化アルゴリズム等への適用に際してより安全性の高い乱数を生成することができる。このため、例えば、より高い安全性が要求される暗号化技術等での使用に適している。

## 請 求 の 範 囲

1. 複数の異なる疑似乱数系列の乱数パターンを出力可能な疑似乱数生成手段と、  
物理乱数を生成する物理乱数生成手段と、  
前記物理乱数生成手段の生成した物理乱数に基づいて前記疑似乱数生成手段の  
出力する乱数の疑似乱数系列を切り替える切替手段と、  
を備える乱数生成装置。
2. 前記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、  
前記切替手段は、前記線形シフトレジスタ符号発生器への帰還入力値の反転／  
非反転を、前記物理乱数生成手段によって生成された物理乱数に基づいて切り替  
えることを特徴とする請求の範囲第1項に記載の乱数生成装置。
3. 前記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、  
前記切替手段は、前記線形シフトレジスタ符号発生器からの出力値の反転／非  
反転を、前記物理乱数生成手段によって生成された物理乱数に基づいて切り替え  
ることを特徴とする請求の範囲第1項に記載の乱数生成装置。
4. 前記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、該線形シ  
フトレジスタ符号発生器のタップの異なる組み合わせに基づく複数の帰還入力値  
を生成し、  
前記切替手段は、前記生成された複数の帰還入力値のうち該線形シフトレジス  
タ符号発生器に帰還入力する帰還入力値を、前記物理乱数生成手段で生成された  
物理乱数に基づいて切り替えることを特徴とする請求の範囲第1項に記載の乱数  
生成装置。

5. 前記疑似乱数生成手段は、所定のタップの組み合わせに基づく第一の帰還入力値を生成する線形シフトレジスタ符号発生器と、該第一の帰還入力値を受け取り前記線形シフトレジスタ符号発生器と同期して所定ビット数ビットシフトを行いその出力を第二の帰還入力値とするフリップフロップと、を含み、

前記切替手段は、前記第一または第二の帰還入力値のうち前記線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、前記物理乱数生成手段で生成された物理乱数に基づいて切り替えることを特徴とする請求の範囲第1項に記載の乱数生成装置。

6. 請求の範囲第2項に記載の乱数生成装置であって、

前記線形シフトレジスタ符号発生器の符号列を検出する検出手段を備え、

前記切替手段は、有効な疑似乱数系列の乱数が前記検出された符号列によっては生成不能である場合には、該疑似乱数系列以外の疑似乱数系列に切り替えることを特徴とする乱数生成装置。

7. 請求の範囲第2項に記載の乱数生成装置であって、

前記線形シフトレジスタ符号発生器の符号列を検出する検出手段と、

有効な疑似乱数系列の乱数が前記検出された符号列によっては生成不能である場合には、前記符号列のビット値のうち少なくとも一つを反転させることを特徴とする乱数生成装置。

図 1

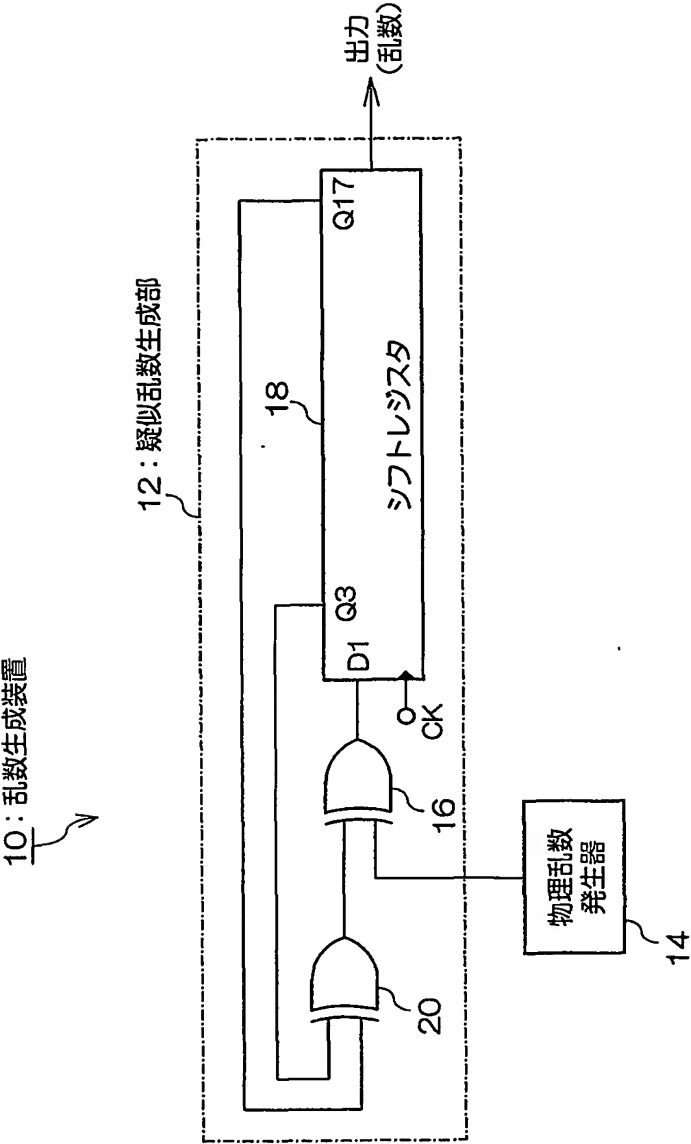


図2

(a)

タイミング	M系列1-1 (物理乱数: 0)	1	2	3	4	FF 5	...	16	17
t(1)	↓	1	1	1	1	1	...	1	1
t(2)	↓	0	1	1	1	1	...	1	1
t(3)	↓	0	0	1	1	1	...	1	1
t(4)	↓	0	0	0	1	1	...	1	1
t(5)	↓	1	0	0	0	1	...	1	1
t(6)	↓	1	1	0	0	0	...	1	1
...	↓			...				...	
t(2 <sup>17</sup> -1)	↓	1	1	1	1	1	...	1	0



(b)

タイミング	M系列1-2 (物理乱数: 1)	1	2	3	4	FF 5	...	16	17
t(1)	↓	0	0	0	0	0	...	0	0
t(2)	↓	1	0	0	0	0	...	0	0
t(3)	↓	1	1	0	0	0	...	0	0
t(4)	↓	1	1	1	0	0	...	0	0
t(5)	↓	0	1	1	1	0	...	0	0
t(6)	↓	0	0	1	1	1	...	0	0
...	↓			...				...	
t(2 <sup>17</sup> -1)	↓	0	0	0	0	0	...	0	1

図3

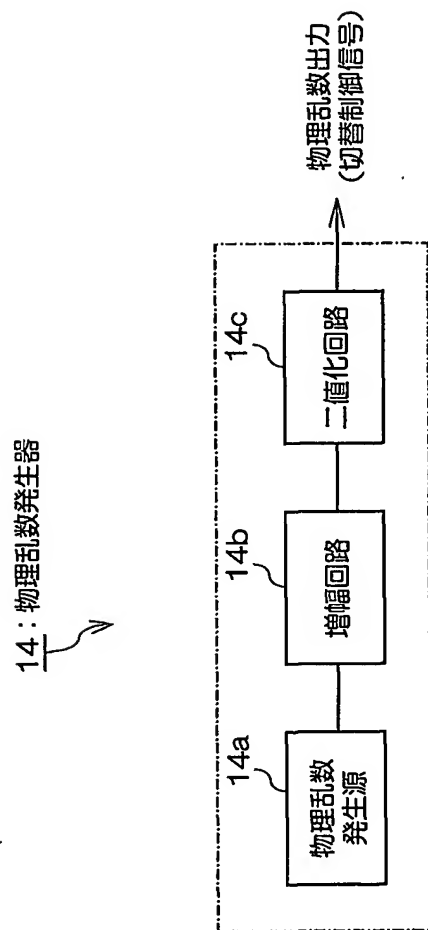


図4

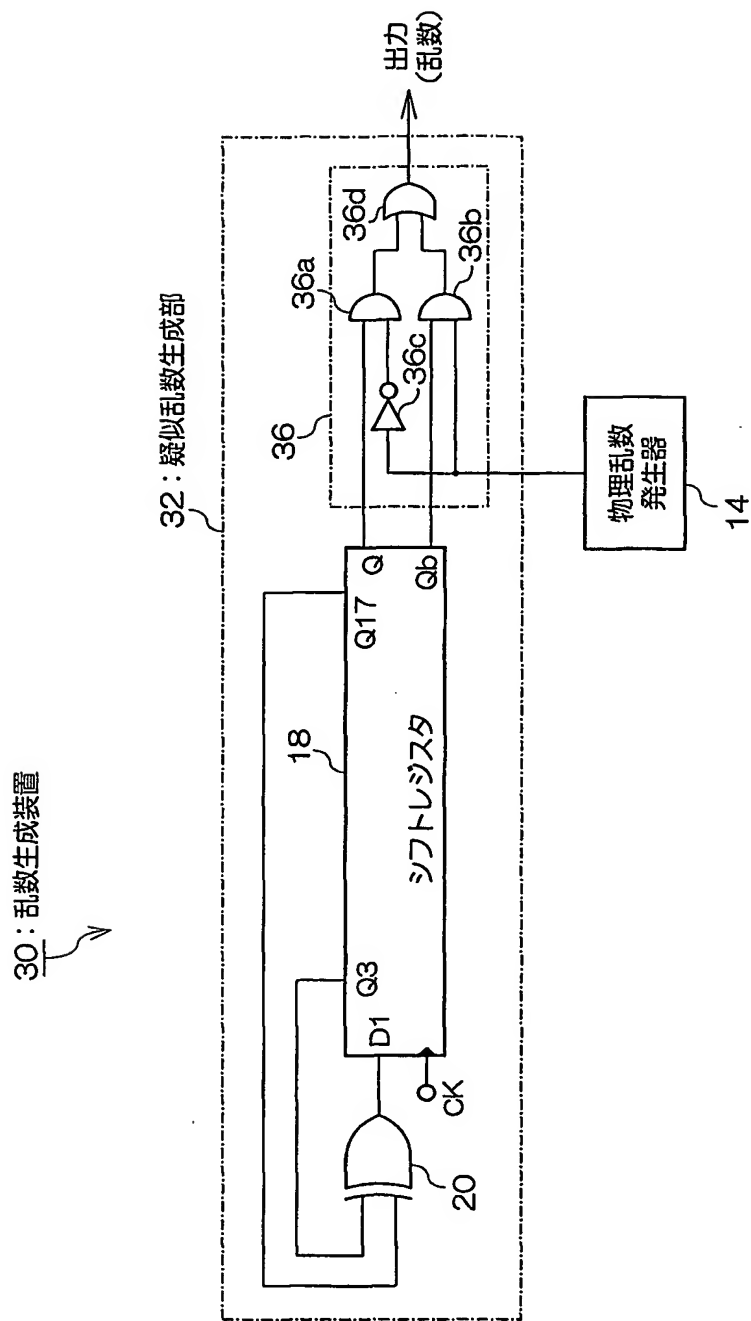


図5

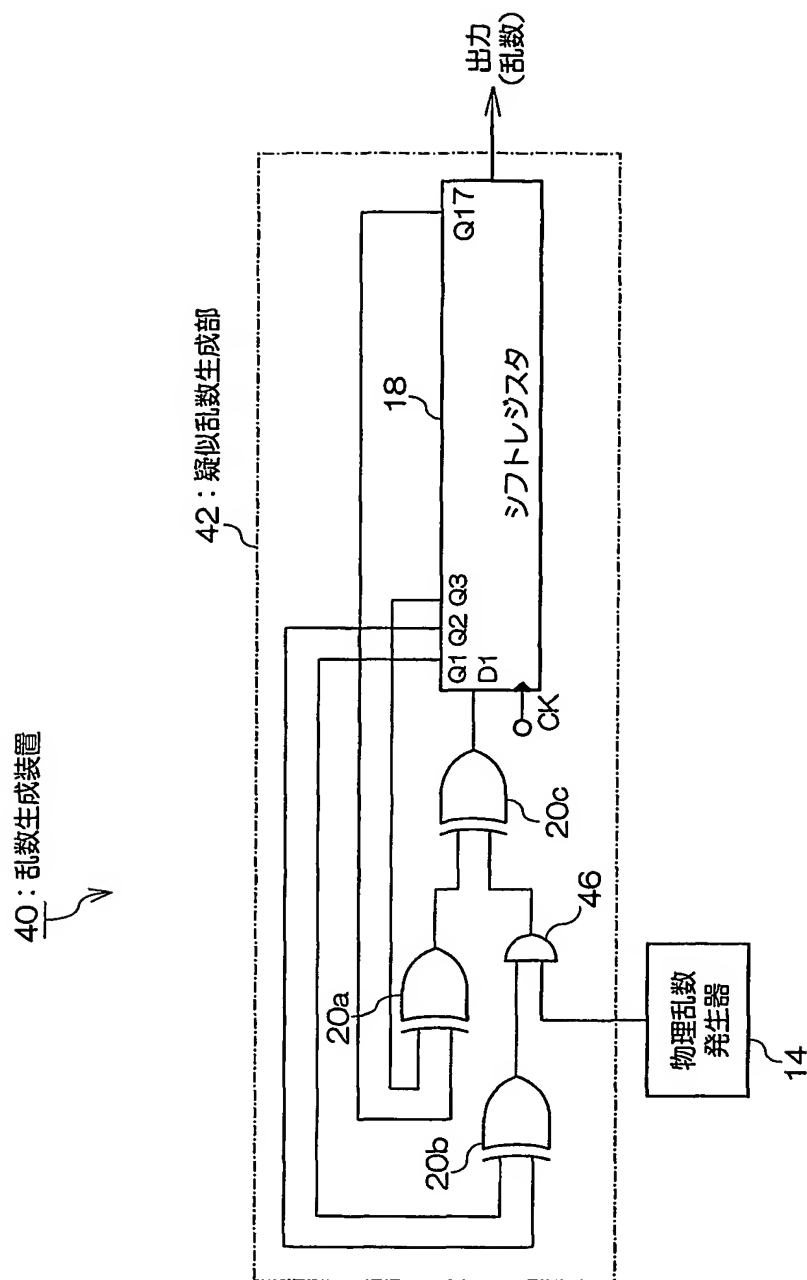
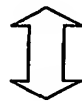




図6

(a)

M系列3-1 (物理乱数: 0)		FF							
		1	2	3	4	5	...	16	17
タイミング	t(1)	1	1	1	1	1	...	1	1
	t(2)	0	1	1	1	1	...	1	1
	t(3)	0	0	1	1	1	...	1	1
	t(4)	0	0	0	1	1	...	1	1
	t(5)	1	0	0	0	1	...	1	1
	t(6)	1	1	0	0	0	...	1	1
	...			...				...	
	t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0



(b)

M系列3-2 (物理乱数: 1)		FF							
		1	2	3	4	5	...	16	17
タイミング	t(1)	1	1	1	1	1	...	1	1
	t(2)	0	1	1	1	1	...	1	1
	t(3)	1	0	1	1	1	...	1	1
	t(4)	0	1	0	1	1	...	1	1
	t(5)	0	0	1	0	1	...	1	1
	t(6)	1	0	0	1	0	...	1	1
	...			...				...	
	t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0

図7

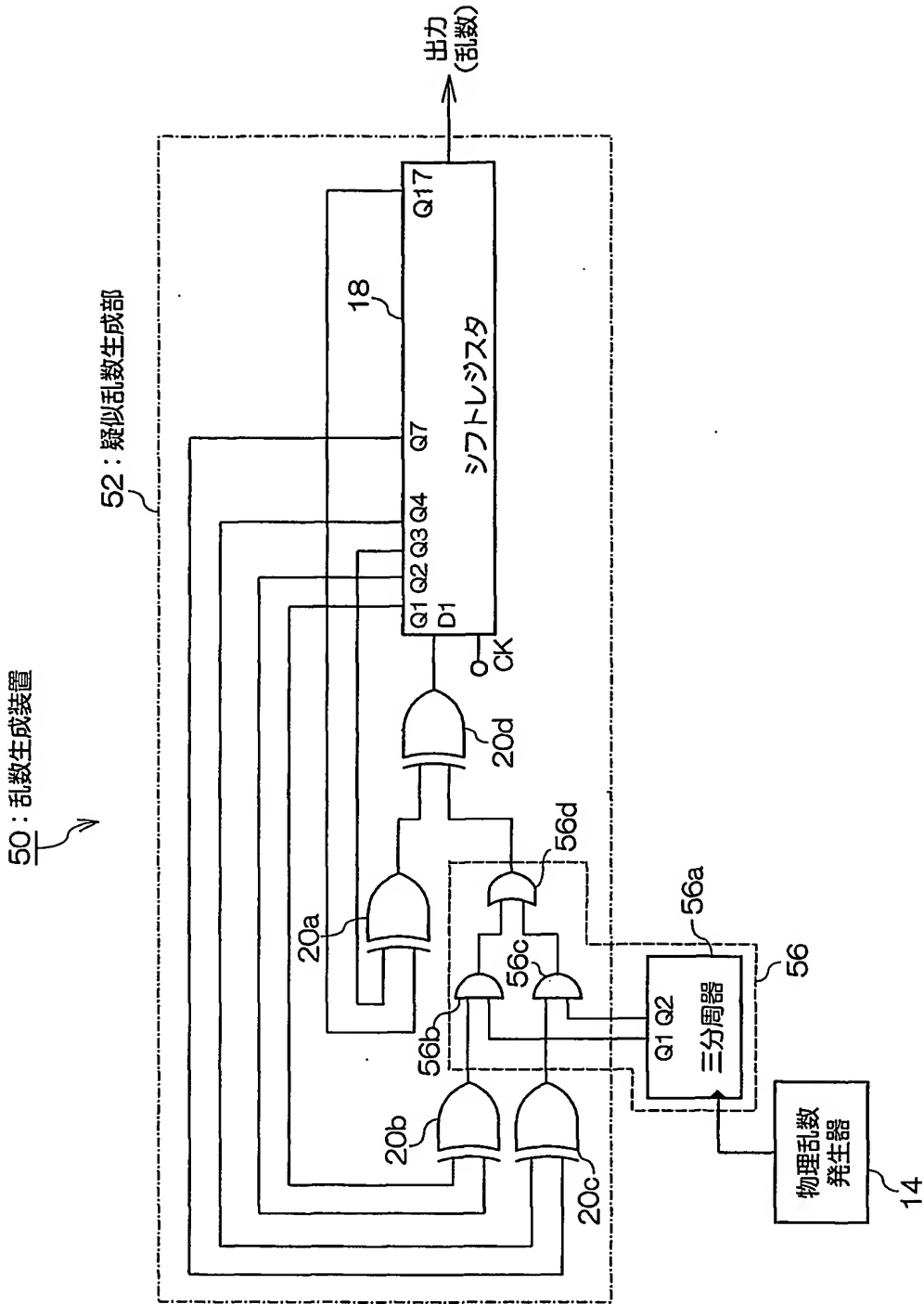


図8

M系列4-1 (Q1=0,Q2=0)		FF								
		1	2	3	4	5	...	16	17	
(a)	タイミング	t(1)	1	1	1	1	1	...	1	1
		t(2)	0	1	1	1	1	...	1	1
		t(3)	0	0	1	1	1	...	1	1
		t(4)	0	0	0	1	1	...	1	1
		t(5)	1	0	0	0	1	...	1	1
		t(6)	1	1	0	0	0	...	1	1
		⋮			⋮					⋮
		t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0
M系列4-2 (Q1=1,Q2=0)		FF								
		1	2	3	4	5	...	16	17	
(b)	タイミング	t(1)	1	1	1	1	1	...	1	1
		t(2)	0	1	1	1	1	...	1	1
		t(3)	1	0	1	1	1	...	1	1
		t(4)	0	1	0	1	1	...	1	1
		t(5)	0	0	1	0	1	...	1	1
		t(6)	0	0	0	1	0	...	1	1
		⋮			⋮					⋮
		t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0
M系列4-3 (Q1=0,Q2=1)		FF								
		1	2	3	4	5	...	16	17	
(c)	タイミング	t(1)	1	1	1	1	1	...	1	1
		t(2)	0	1	1	1	1	...	1	1
		t(3)	0	0	1	1	1	...	1	1
		t(4)	0	0	0	1	1	...	1	1
		t(5)	1	0	0	0	1	...	1	1
		t(6)	0	1	0	0	0	...	1	1
		⋮			⋮					⋮
		t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0

図9

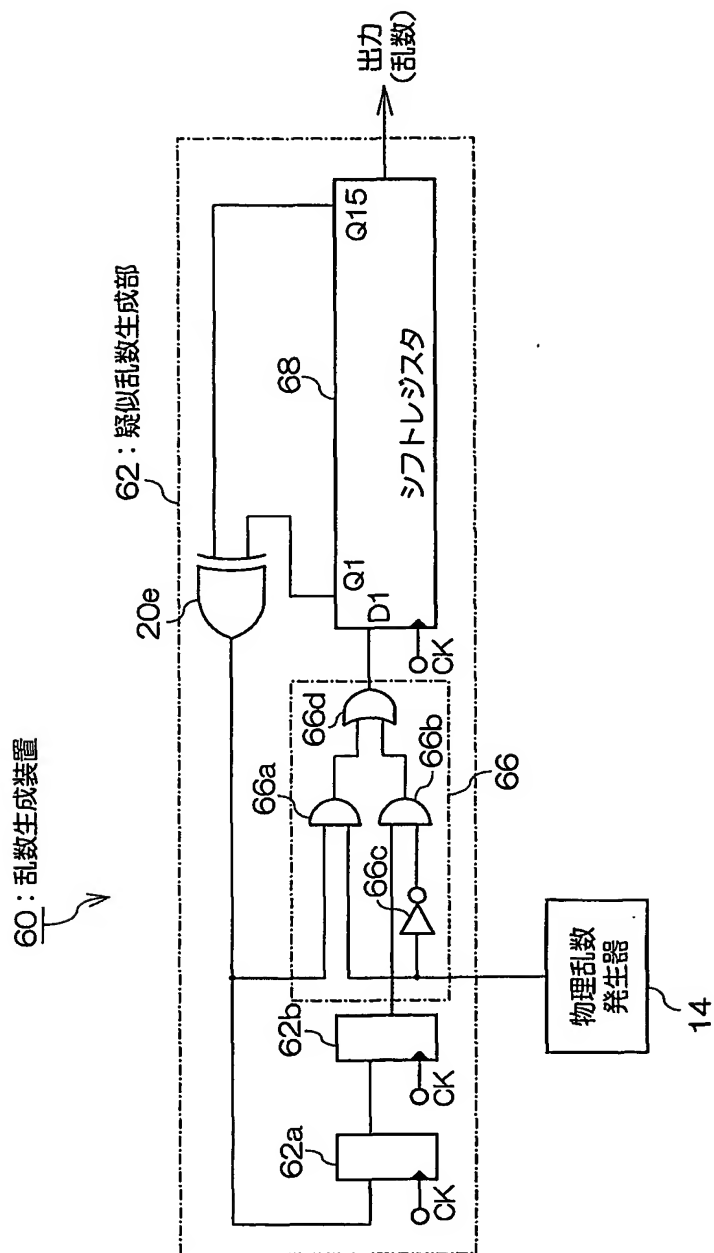


図10

(a)

M系列5-1 (物理乱数:0)	FF							
	1	2	3	4	5	...	16	17
↓ t(1)	1	1	1	1	1	...	1	1
↓ t(2)	0	1	1	1	1	...	1	1
↓ t(3)	0	0	1	1	1	...	1	1
↓ t(4)	0	0	0	1	1	...	1	1
↓ t(5)	1	0	0	0	1	...	1	1
↓ t(6)	1	1	0	0	0	...	1	1
↓ ...			...				...	
↓ t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0

タイミング

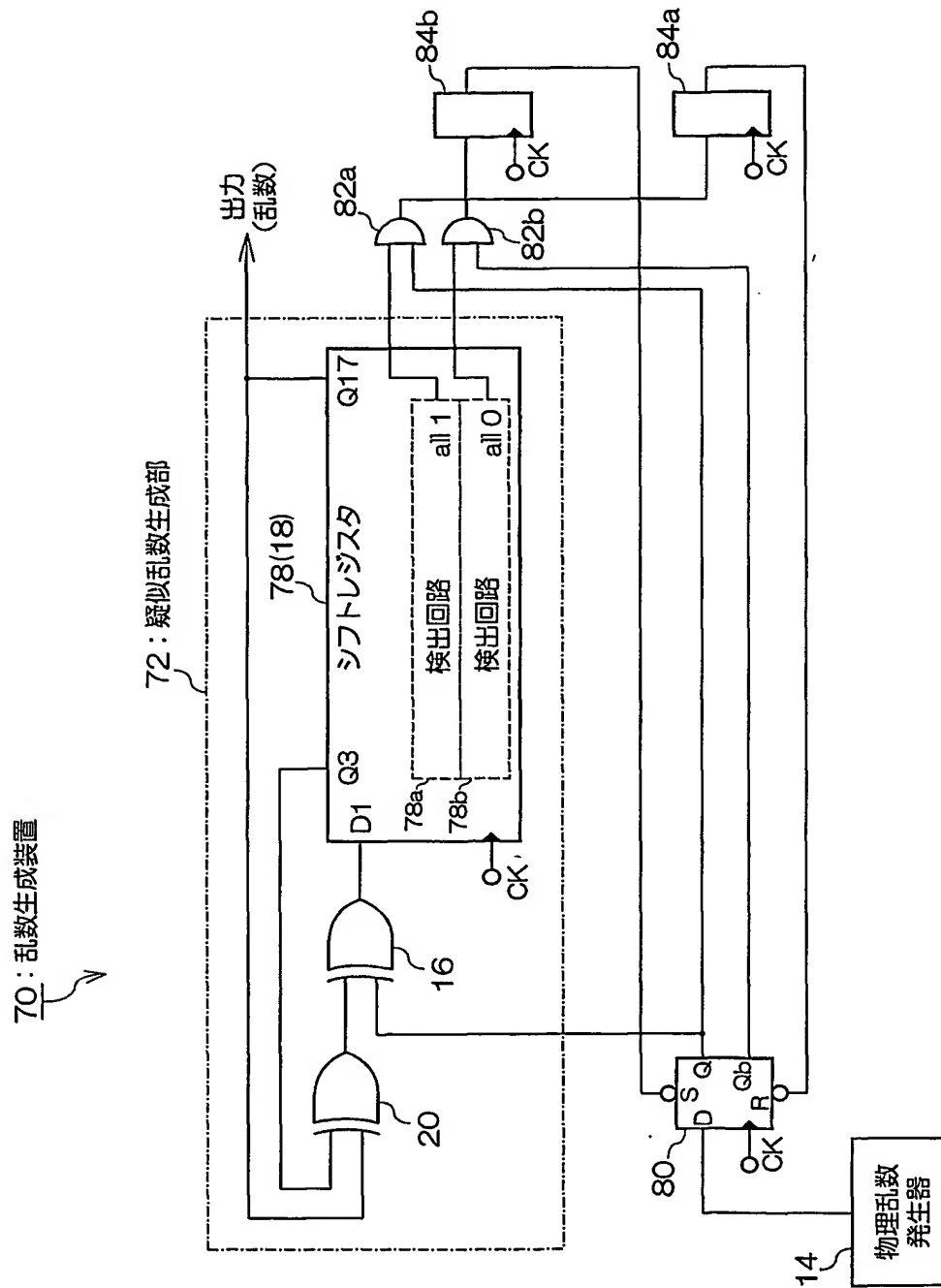


(b)

M系列5-2 (物理乱数:1)	FF							
	1	2	3	4	5	...	14	15
↓ t(1)	1	1	1	1	1	...	1	1
↓ t(2)	0	1	1	1	1	...	1	1
↓ t(3)	1	0	1	1	1	...	1	1
↓ t(4)	0	1	0	1	1	...	1	1
↓ t(5)	1	0	1	0	1	...	1	1
↓ t(6)	1	1	0	1	0	...	1	1
↓ ...			...				...	
↓ t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0

タイミング

図 11



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/14055

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L9/24, G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> H04L9/24, G06F7/58Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004  
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Microfilm of the specification and drawings annexed to the request of Japanese Utility Model Application No. 54192/1980 (Laid-open No. 156134/1981) (Nikoo-Electronics Co., Ltd.), 21 November, 1981 (21.11.81), Full text; Figs. 1 to 2 (Family: none)	1-7
Y	JP 10-262041 A (International Business Machines Corp.), 29 September, 1998 (29.09.98), Par. No. [0018]; Fig. 1 & US 6282291 B	1-7

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
03 February, 2004 (03.02.04)Date of mailing of the international search report  
17 February, 2004 (17.02.04)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/14055

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 8-503569 A (Motorola, Inc.), 16 April, 1996 (16.04.96), Page 11, line 28 to page 13, line 20; Fig. 2 & DE 69429157 D & US 5365585 A & CA 2146439 A & WO 95/06906 A & FI 951946 A & GB 2286274 A & HK 1002338 A & KR 168504 B & BR 9405567 A & SG 76452 A & EP 672273 A & DE 69429157 T	2, 4-7
Y	JP 9-509748 A (RAIKE, William, Michael), 30 September, 1997 (30.09.97), Page 28, line 25 to page 30, line 22; Fig. 1 & AU 1204995 A & AU 1132199 A & WO 95/15633 A & EP 734624 A & NZ 277128 A & US 5799088 A & NZ 329808 A & NZ 336413 A & NZ 336414 A & AU 729638 B & JP 2002-314534 A & JP 3339688 B	3



## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/24 G06F7/58

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/24 G06F7/58

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2004年

日本国登録実用新案公報 1994-2004年

日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	日本国実用新案登録出願55-54192号 (日本国実用新案登録出願公開56-156134号) の願書に添付した明細書及び図面の内容を記録したマイクロフィルム (ニコー電子株式会社) 1981. 11. 21, 全文, 第1-2図 (ファミリーなし).	1-7
Y	JP 10-262041 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 1998. 09. 29, 第【0018】段落, 図1 & US 6282291 B	1-7

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行者若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

03. 02. 2004

国際調査報告の発送日

17. 2. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	<p>JP 8-503569 A (モトローラ・インコーポレイテッド)</p> <p>1996.04.16</p> <p>第11頁第28行-第13頁第20行, 図2</p> <p>&amp; DE 69429157 D</p> <p>&amp; US 5365585 A &amp; CA 2146439 A</p> <p>&amp; WO 95/06906 A &amp; FI 951946 A</p> <p>&amp; GB 2286274 A &amp; HK 1002338 A</p> <p>&amp; KR 168504 B &amp; BR 9405567 A</p> <p>&amp; SG 76452 A &amp; EP 672273 A</p> <p>&amp; DE 69429157 T</p>	2, 4-7
Y	<p>JP 9-509748 A (ライク, ウィリアム, マイケル)</p> <p>1997.09.30</p> <p>第28頁第25行-第30頁第22行, FIG. 1</p> <p>&amp; AU 1204995 A &amp; AU 1132199 A</p> <p>&amp; WO 95/15633 A &amp; EP 734624 A</p> <p>&amp; NZ 277128 A &amp; US 5799088 A</p> <p>&amp; NZ 329808 A &amp; NZ 336413 A</p> <p>&amp; NZ 336414 A &amp; AU 729638 B</p> <p>&amp; JP 2002-314534 A</p> <p>&amp; JP 3339688 B</p>	3

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/JP03/14055

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L9/24, G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> H04L9/24, G06F7/58

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004  
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Microfilm of the specification and drawings annexed to the request of Japanese Utility Model Application No. 54192/1980 (Laid-open No. 156134/1981) (Nikoo-Electronics Co., Ltd.), 21 November, 1981 (21.11.81), Full text; Figs. 1 to 2 (Family: none)	1-7
Y	JP 10-262041 A (International Business Machines Corp.), 29 September, 1998 (29.09.98), Par. No. [0018]; Fig. 1 & US 6282291 B	1-7

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
03 February, 2004 (03.02.04)

Date of mailing of the international search report  
17 February, 2004 (17.02.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/14055

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 8-503569 A (Motorola, Inc.), 16 April, 1996 (16.04.96), Page 11, line 28 to page 13, line 20; Fig. 2 & DE 69429157 D & US 5365585 A & CA 2146439 A & WO 95/06906 A & FI 951946 A & GB 2286274 A & HK 1002338 A & KR 168504 B & BR 9405567 A & SG 76452 A & EP 672273 A & DE 69429157 T	2, 4-7
Y	JP 9-509748 A (RAIKE, William, Michael), 30 September, 1997 (30.09.97), Page 28, line 25 to page 30, line 22; Fig. 1 & AU 1204995 A & AU 1132199 A & WO 95/15633 A & EP 734624 A & NZ 277128 A & US 5799088 A & NZ 329808 A & NZ 336413 A & NZ 336414 A & AU 729638 B & JP 2002-314534 A & JP 3339688 B	3